

Ex. E - Claim Chart

U.S. Patent No. 9,600,661



US009600661B2

(12) **United States Patent**
Safa

(10) **Patent No.:** **US 9,600,661 B2**
(45) **Date of Patent:** **Mar. 21, 2017**

(54) **SYSTEM AND METHOD TO SECURE A COMPUTER SYSTEM BY SELECTIVE CONTROL OF WRITE ACCESS TO A DATA STORAGE MEDIUM**

FOREIGN PATENT DOCUMENTS

GB 2407515 A * 12/2004
JP 08044630 A 2/1996
(Continued)

(75) Inventor: **John Safa**, Nottingham (GB)

OTHER PUBLICATIONS

(73) Assignee: **Drive Sentry Limited**, Berkshire (GB)

FileMerlin? Conversion Library and API for Developers [online]. Advanced Computer Innovations, Inc., 2004 [retrieved on Jan. 28, 2008]. Retrieved from the Internet: <URL: http://web.archive.org/web/20040810113019/file-convert.com/fndvref.htm>.*

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 503 days.

(Continued)

(21) Appl. No.: **11/292,910**

Primary Examiner — Larry Mackall
(74) Attorney, Agent, or Firm — Ted Sabety; Sabety +associates, PLLC

(22) Filed: **Dec. 1, 2005**

(65) **Prior Publication Data**

US 2007/0130433 A1 Jun. 7, 2007

ABSTRACT

(51) **Int. Cl.**

G06F 12/00 (2006.01)

G06F 21/52 (2013.01)

(52) **U.S. Cl.**

CPC **G06F 21/52** (2013.01)

(58) **Field of Classification Search**

CPC **G06F 12/14**; **G06F 21/52**

USPC 711/163

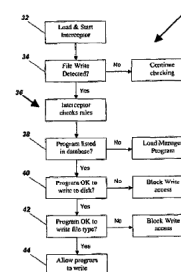
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,825,877 A 10/1998 Dan et al.
5,974,549 A * 10/1999 Golan 726/23
6,308,274 B1 10/2001 Swift
6,922,781 B1 * 7/2005 Shuster 713/165
6,941,470 B1 9/2005 Joostie
6,978,366 B1 * 12/2005 Ignatchenko et al. 713/166
7,681,237 B1 * 3/2010 Spiegel 726/24
(Continued)

58 Claims, 3 Drawing Sheets



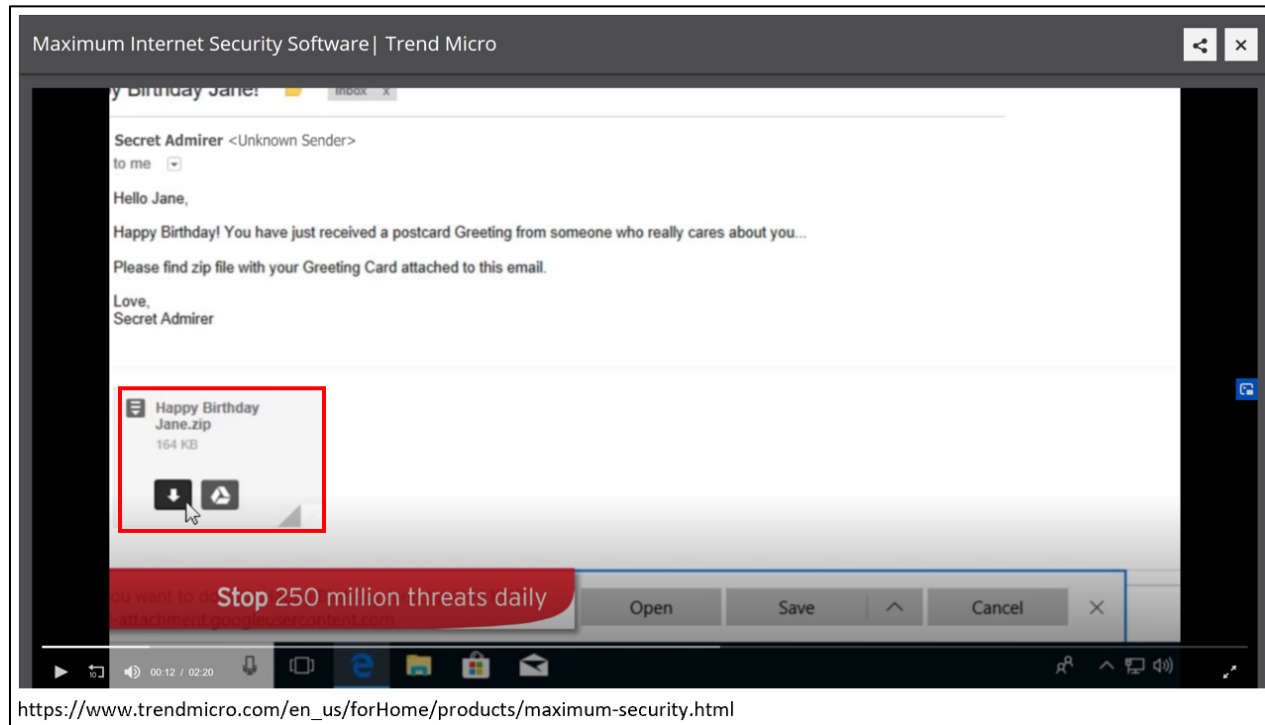
Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	TREND MICRO PRODUCTS
<p>16[pre] In a computer comprising a mass data storage device and an application running on said computer in conjunction with an operating system that manages access to said data storage device, a method of controlling write access to said data storage device by said application comprising:</p>	<p>Trend Micro offers various software that performs the method of claim 16. Specifically, Trend Micro offers many applications to protect against electronic threats such as viruses, ransomware, malware, and the like (collectively “hostile applications”). That software includes but is not limited to, OfficeScan, Endpoint Application Control, Apex One, Antivirus+ Security, Internet Security, and Maximum Security.</p> <p>Trend Micro’s software operates and run on a computer such as a PC, Mac, or Server with a mass data storage device such as a hard disk or memory. The software controls write access to the computer’s storage device by a hostile application running on the computer. As illustrated in the graphic below, Trend Micro’s applications allow safe files while blocking malicious files.</p> <div data-bbox="600 738 1806 1341"> <p>LEGEND</p> <ul style="list-style-type: none"> Known Good Data (white circle) Known Bad Data (black circle) Unknown Data (grey circle) Noise Cancellation (speaker icon with a slash) <p>Safe files allowed</p> <p>Malicious files blocked</p> <p>Web and File Reputation Exploit Prevention Application Control Variant Protection</p> <p>Pre-execution Machine Learning</p> <p>Behavioral Analysis Runtime Machine Learning</p> <p>Custom Sandbox Analysis</p> <p>Investigation & Response</p> <p>Datasheet, Trend Micro Office Scan, at 2</p> </div>

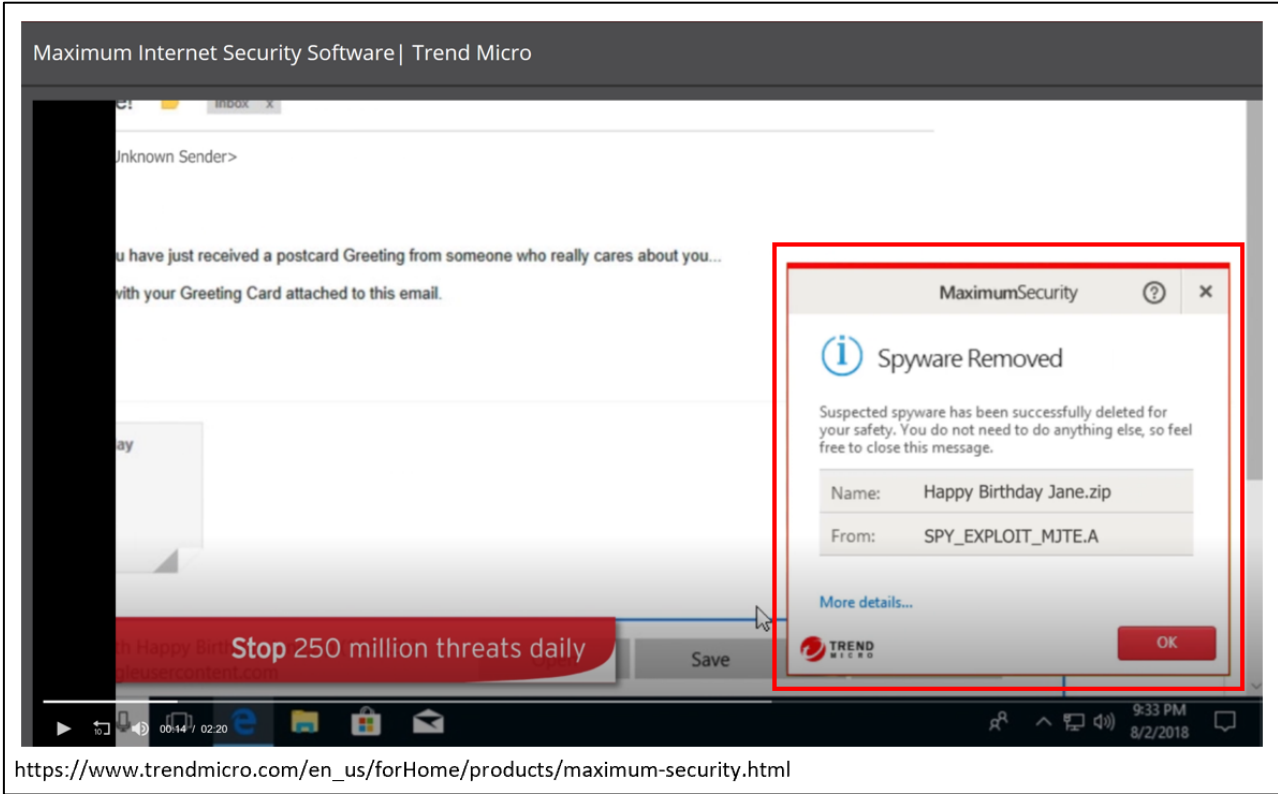
Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	TREND MICRO PRODUCTS
<p>16[pre] In a computer comprising a mass data storage device and an application running on said computer in conjunction with an operating system that manages access to said data storage device, a method of controlling write access to said data storage device by said application comprising:</p>	<p>Trend Micro’s software detects write attempts and controls write access to the data storage device during every stage of the hostile application’s presence: (1) entry-point; (2) pre-execution; (3) runtime; and (4) exit point. The graphic below showing how Trend Micro’s software defends endpoints (e.g., the claimed “computer”) is illustrative. First, when the hostile application arrives on an endpoint via for example a network, email, or USB, the software will detect write attempts and control write access. Second, while malware is being written to the storage medium, but before execution, the software detects write attempts and controls write access. Third, while the application is running it can make attempts to write data, which the software will detect and control. Fourth, when the applications exits it can make attempt to write data, which the software will also detect and control.</p> <div data-bbox="730 738 1707 1386" style="border: 1px solid black; padding: 10px; margin: 10px auto; width: 80%;"> <p style="text-align: center; font-size: 1.2em;">How it works</p> <p style="text-align: center;">A range of layered detection capabilities, alongside investigation and response, defends the endpoint <u>through every stage</u></p> <p style="text-align: center; font-size: 0.8em;"> https://www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint.html </p> </div>

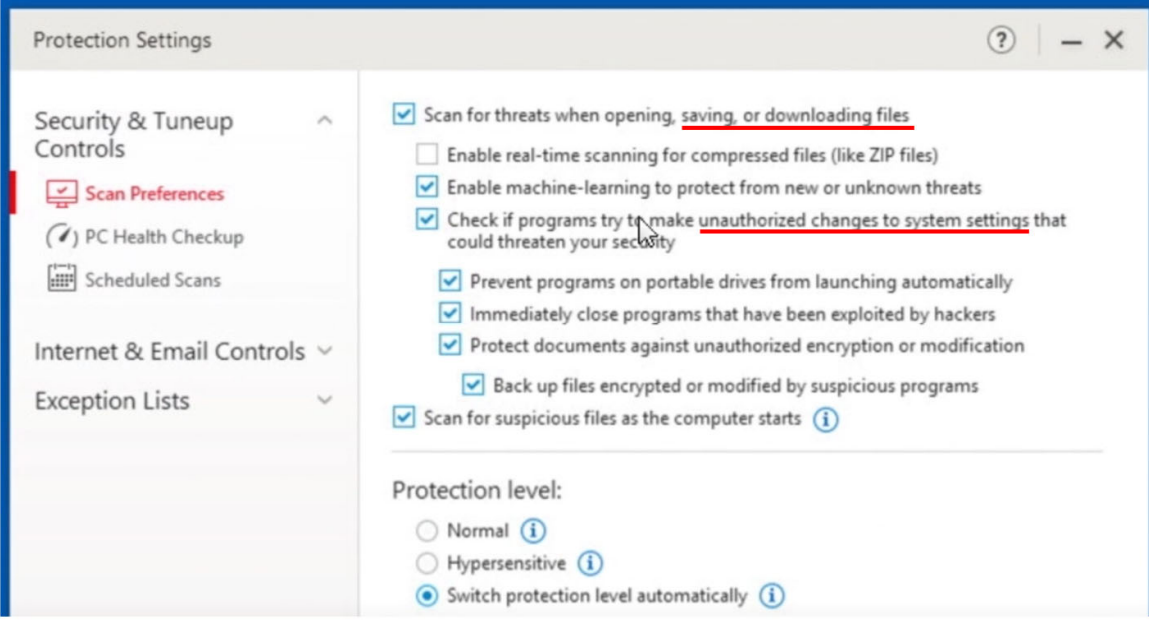
Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	TREND MICRO PRODUCTS
<p>16[pre] In a computer comprising a mass data storage device and an application running on said computer in conjunction with an operating system that manages access to said data storage device, a method of controlling write access to said data storage device by said application comprising:</p>	<p>The remaining slides for limitation 16[pre] provide examples of Trend Micro's software detecting write attempts and controlling the write access of hostile applications.</p> <p>The example on this slide shows Trend Micro's Maximum Security software detecting a write attempt and controlling write access by an email attachment. In the image below, the user attempts to and or downloads a zip file from an email attachment, which would cause data to be written to the storage medium. In the image on the next slide, Trend Micro's software detects and rejects that attempt to write.</p> <div data-bbox="588 654 1845 1375">  <p>Maximum Internet Security Software Trend Micro</p> <p>Happy Birthday Jane!</p> <p>Secret Admirer <Unknown Sender> to me</p> <p>Hello Jane,</p> <p>Happy Birthday! You have just received a postcard Greeting from someone who really cares about you...</p> <p>Please find zip file with your Greeting Card attached to this email.</p> <p>Love, Secret Admirer</p> <p>Happy Birthday Jane.zip 164 KB</p> <p>Download Save</p> <p>Stop 250 million threats daily</p> <p>Open Save Cancel</p> <p>https://www.trendmicro.com/en_us/forHome/products/maximum-security.html</p> </div>

Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	TREND MICRO PRODUCTS
<p>16[pre] In a computer comprising a mass data storage device and an application running on said computer in conjunction with an operating system that manages access to said data storage device, a method of controlling write access to said data storage device by said application comprising:</p>	<p>The image below shows that Trend Micro's software detects and rejects that attempt to write before the user has clicked to save the file.</p>  <p>https://www.trendmicro.com/en_us/forHome/products/maximum-security.html</p>

Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	TREND MICRO PRODUCTS
<p>16[pre] In a computer comprising a mass data storage device and an application running on said computer in conjunction with an operating system that manages access to said data storage device, a method of controlling write access to said data storage device by said application comprising:</p>	<p>The image below shows another example of Trend Micro’s Security software’s ability to detect write attempts and control write access to a storage device. As the image shows, the software scans for threats when saving or downloading files or when programs try to make unauthorized changes to system settings for the purpose of preventing write access.</p> <div data-bbox="577 500 1759 1174">  <p>https://www.trendmicro.com/en_us/forHome/products/maximum-security.html</p> </div> <div data-bbox="598 1203 1556 1401" style="border: 1px solid black; padding: 5px;"> <p>2. The following Scan Preferences are displayed. Check or uncheck to change a setting.</p> <ul style="list-style-type: none"> • <u>Scan for threats when opening, saving, or downloading suspicious files.</u> This is the real-time scan that protects you at all times when you’re using your computer. This is enabled by default. <p style="font-size: small;">Trend Micro Security 2020 for Windows Product Guide at 72.</p> </div>

Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	TREND MICRO PRODUCTS
<p>16[pre] In a computer comprising a mass data storage device and an application running on said computer in conjunction with an operating system that manages access to said data storage device, a method of controlling write access to said data storage device by said application comprising:</p>	<p>The image below shows another example of Trend Micro’s Security software’s ability to detect write attempts and control write access to a storage device. As the image shows, threats are caught as they try to enter memory or touch the hard drive.</p> <div data-bbox="573 566 1892 862" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Quick Start: Conducting On-Demand Scans</p> <p>By default, Trend Micro Security activates a real-time scan when it is installed. This is always present in memory, to proactively protect you from real-time threats. <u>Threats are caught as they try to enter memory or touch the hard drive</u>, preventing infections. This includes protection against ransomware, which may infect you from dangerous websites or emails.</p> <p><small>Trend Micro Security 2020 for Windows Product Guide at 60.</small></p> </div>







Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	TREND MICRO PRODUCTS				
<p>16[pre] In a computer comprising a mass data storage device and an application running on said computer in conjunction with an operating system that manages access to said data storage device, a method of controlling write access to said data storage device by said application comprising:</p>	<p>Trend Micro's OfficeScan and ApexOne software also include real-time scans, which detect write attempts and control write access of hostile applications. For example, the software scans files whose contents are being written, and will reject write access if the application is hostile.</p> <div data-bbox="583 505 1677 899"> <p>Real-time Scan: Advanced Settings</p> <table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td>Scan Trigger</td><td> <ul style="list-style-type: none"> • Read: Scans files whose contents are read; files are read when they are opened, executed, copied, or moved. • Write: Scans files whose contents are being written; a file's contents are written when the file is modified, saved, downloaded, or copied from another location. • Read or write </td></tr> </tbody> </table> <p>https://docs.trendmicro.com/all/ent/officescan/v11.0/en-us/osce_11.0_agent_olh/scn_adv_sttng_rltm_osce_agent.html (Office Scan Agent)</p> </div> <div data-bbox="583 940 1587 1367"> <p><u>Real-time Scan</u></p> <p>Real-time Scan is a persistent and ongoing scan. <u>Each time a file is received, opened, downloaded, copied, or modified, Real-time Scan scans the file for security risks.</u> If the Security Agent does not detect a security risk, users can proceed to access the file. If the Security Agent detects a security risk or a probable virus/malware, a notification message displays indicating the name of the infected file and the specific security risk.</p> <p>Real-time Scan maintains a persistent scan cache which reloads each time the Security Agent starts. The Security Agent tracks any changes to files or folders that occurred since the Security Agent unloaded and removes these files from the cache.</p> <p>Trend Micro Apex One Administrator's Guide at 7-14</p> </div>	Option	Description	Scan Trigger	<ul style="list-style-type: none"> • Read: Scans files whose contents are read; files are read when they are opened, executed, copied, or moved. • Write: Scans files whose contents are being written; a file's contents are written when the file is modified, saved, downloaded, or copied from another location. • Read or write
Option	Description				
Scan Trigger	<ul style="list-style-type: none"> • Read: Scans files whose contents are read; files are read when they are opened, executed, copied, or moved. • Write: Scans files whose contents are being written; a file's contents are written when the file is modified, saved, downloaded, or copied from another location. • Read or write 				


Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	TREND MICRO PRODUCTS
<p>16[pre] In a computer comprising a mass data storage device and an application running on said computer in conjunction with an operating system that manages access to said data storage device, a method of controlling write access to said data storage device by said application comprising:</p>	<p>Trend Micro’s software also includes Behavior Monitoring that detects write attempts and controls write access of hostile applications. As explained in the excerpt below, Behavior Monitoring constantly monitors endpoints, e.g., the claimed computers, for unusual modifications to the operating system or on installed software. That monitoring occurs for the purpose of detecting write attempts by hostile applications and controlling their write access.</p> <div data-bbox="577 592 1837 1031" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p><u>Behavior Monitoring</u></p> <p>Behavior Monitoring constantly monitors endpoints for unusual modifications to the operating system or on installed software. Behavior Monitoring protects endpoints through Malware Behavior Blocking and Event Monitoring. Complementing these two features are a user-configured exception list and the Certified Safe Software Service.</p> <p>Office Scan, Service Pack 1, Administrator’s Guide at 9-2</p> </div>

Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	TREND MICRO PRODUCTS				
<p>16[pre] In a computer comprising a mass data storage device and an application running on said computer in conjunction with an operating system that manages access to said data storage device, a method of controlling write access to said data storage device by said application comprising:</p>	<p>The Behavior Monitoring service includes ransomware protection that detects attempts by applications to modify, delete, or rename files or in the modification of the file type. If the software detects any of those attempts, it terminates and attempts to quarantine the hostile applications, thereby controlling write access.</p> <table border="1" data-bbox="766 503 1575 1339"> <thead> <tr> <th data-bbox="772 508 972 557">OPTION</th><th data-bbox="972 508 1568 557">DESCRIPTION</th></tr> </thead> <tbody> <tr> <td data-bbox="772 557 972 1334"> Protect documents against unauthorized encryption or modification </td><td data-bbox="972 557 1568 1334"> <p>You can configure Behavior Monitoring to detect a specific sequence of events that may indicate a ransomware attack. After Behavior Monitoring matches all of the following criteria, the OfficeScan agent terminates and attempts to quarantine malicious programs:</p> <ol style="list-style-type: none"> 1. A process not recognized as safe attempts to modify, delete, or rename three files within a certain time interval. 2. The process attempted to modify a protected file extension type <p>Additionally enable Automatically back up files changed by suspicious programs to create copies of files being encrypted on endpoints. After the encryption process completes and OfficeScan detects a ransomware threat, OfficeScan prompts end users to restore the affected files without suffering any loss of data.</p> <hr/> <p> Note</p> <p>Automatic file backup requires at least 100 MB of disk space on the agent endpoint and only backs up files that are less than 10 MB in size.</p> <p>The backup folder location on agent endpoints is: <Agent installation folder>\CCSF\module\DRE\data.</p> <hr/> <p> WARNING!</p> <p>If Automatically back up files changed by suspicious programs is not enabled, OfficeScan cannot recover the first files affected by a ransomware threat.</p> </td></tr> </tbody> </table> <p>Office Scan, Service Pack 1, Administrator's Guide at 9-4</p>	OPTION	DESCRIPTION	Protect documents against unauthorized encryption or modification	<p>You can configure Behavior Monitoring to detect a specific sequence of events that may indicate a ransomware attack. After Behavior Monitoring matches all of the following criteria, the OfficeScan agent terminates and attempts to quarantine malicious programs:</p> <ol style="list-style-type: none"> 1. A process not recognized as safe attempts to modify, delete, or rename three files within a certain time interval. 2. The process attempted to modify a protected file extension type <p>Additionally enable Automatically back up files changed by suspicious programs to create copies of files being encrypted on endpoints. After the encryption process completes and OfficeScan detects a ransomware threat, OfficeScan prompts end users to restore the affected files without suffering any loss of data.</p> <hr/> <p> Note</p> <p>Automatic file backup requires at least 100 MB of disk space on the agent endpoint and only backs up files that are less than 10 MB in size.</p> <p>The backup folder location on agent endpoints is: <Agent installation folder>\CCSF\module\DRE\data.</p> <hr/> <p> WARNING!</p> <p>If Automatically back up files changed by suspicious programs is not enabled, OfficeScan cannot recover the first files affected by a ransomware threat.</p>
OPTION	DESCRIPTION				
Protect documents against unauthorized encryption or modification	<p>You can configure Behavior Monitoring to detect a specific sequence of events that may indicate a ransomware attack. After Behavior Monitoring matches all of the following criteria, the OfficeScan agent terminates and attempts to quarantine malicious programs:</p> <ol style="list-style-type: none"> 1. A process not recognized as safe attempts to modify, delete, or rename three files within a certain time interval. 2. The process attempted to modify a protected file extension type <p>Additionally enable Automatically back up files changed by suspicious programs to create copies of files being encrypted on endpoints. After the encryption process completes and OfficeScan detects a ransomware threat, OfficeScan prompts end users to restore the affected files without suffering any loss of data.</p> <hr/> <p> Note</p> <p>Automatic file backup requires at least 100 MB of disk space on the agent endpoint and only backs up files that are less than 10 MB in size.</p> <p>The backup folder location on agent endpoints is: <Agent installation folder>\CCSF\module\DRE\data.</p> <hr/> <p> WARNING!</p> <p>If Automatically back up files changed by suspicious programs is not enabled, OfficeScan cannot recover the first files affected by a ransomware threat.</p>				

Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	TREND MICRO PRODUCTS
<p>16[pre] In a computer comprising a mass data storage device and an application running on said computer in conjunction with an operating system that manages access to said data storage device, a method of controlling write access to said data storage device by said application comprising:</p>	<p>The following excerpt shows that Apex One also includes Behavior Monitoring functionality.</p> <div data-bbox="674 444 1644 899" style="border: 1px solid black; padding: 10px; margin: 10px auto; width: 80%;"> <p><u>Behavior Monitoring</u></p> <p>Behavior Monitoring constantly monitors endpoints for unusual modifications to the operating system or on installed software. Behavior Monitoring protects endpoints through Malware Behavior Blocking and Event Monitoring. Complementing these two features are a user-configured exception list and the Certified Safe Software Service.</p> <hr/> <p> Important</p> <p>By default, Behavior Monitoring is disabled on all versions of Windows Server platforms.</p> <hr/> <p>Trend Micro Apex One Administrator's Guide at 9-2</p> </div>

Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	TREND MICRO PRODUCTS
<p>16[pre] In a computer comprising a mass data storage device and an application running on said computer in conjunction with an operating system that manages access to said data storage device, a method of controlling write access to said data storage device by said application comprising:</p>	<p>The following excerpt shows that Trend Micro’s Security software (Antivirus+ Security, Internet Security, and Maximum Security) also includes Behavior Monitoring functionality.</p> <div data-bbox="709 448 1474 802" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p style="color: red; text-align: center;">Trend Micro Security 2020 for Windows Product Guide</p> <p>Trend Micro™ <u>Antivirus+ Security</u></p> <p>Trend Micro™ <u>Internet Security</u></p> <p>Trend Micro™ <u>Maximum Security</u></p> <p>Trend Micro Security 2020 for Windows Product Guide at 1.</p> </div> <div data-bbox="709 889 1797 1305" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Unauthorized Change Prevention</p> <p>Trend Micro Security includes <u>behavior monitoring</u> in its list of security protections. Unauthorized changes to system settings and other suspicious behavior can be blocked, as well as autorun programs on portable drives. Antivirus+ includes the ability to switch your protection level automatically, to aggressively eliminate programs that pose even a small risk of bad behavior. And the increased protection against ransomware that Folder Shield provides helps protect your computer and files from encryption or blocked access and the extortion that comes with ransomware. All editions of Trend Micro Security provide ransomware protection and Folder Shield.</p> <p>Trend Micro Security 2020 for Windows Product Guide at 70.</p> </div>

Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	TREND MICRO PRODUCTS
<p>16[pre] In a computer comprising a mass data storage device and an application running on said computer in conjunction with an operating system that manages access to said data storage device, a method of controlling write access to said data storage device by said application comprising:</p>	<p>Trend Micro's Endpoint Application Control software also controls write access of hostile applications. Endpoint Application Control detects write attempt to prevent them from occurring. For example it detects and prevents write attempts by executables, DLLs, Windows App store apps, device drivers, controls panels, and other portable executable files.</p> <div data-bbox="655 521 1713 829" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Trend Micro Endpoint Application Control allows you to enhance your defenses against malware and targeted attacks by <u>preventing unknown and unwanted applications from executing on your corporate endpoints</u>. With a combination of flexible, dynamic policies, whitelisting and blacklisting capabilities, as well as an extensive application catalog, this easy-to-manage solution significantly reduces your endpoint attack exposure. For even greater insight into threats, user-based visibility and policy management are available in the local administration console or in the centrally-managed Trend Micro™ Control Manager™.</p> <p><small>Datasheet, Trend Micro Endpoint Application Control, at 1</small></p> </div> <div data-bbox="655 873 1299 1330" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Enhanced protection defends against malware, targeted attacks, and zero-day threats</p> <ul style="list-style-type: none"> • <u>Prevents potential damage from unwanted or unknown applications (executables, DLLs, Windows App store apps, device drivers, control panels, and other Portable Executable (PE) files)</u> • Provides global and local real-time threat intelligence based on good file reputation data correlated across a global network <p><small>Datasheet, Trend Micro Endpoint Application Control, at 1</small></p> </div>

Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	TREND MICRO PRODUCTS								
<p>16[a] detecting using a process operating in kernel mode monitoring file system access an attempt by the application to write data of a designated file type to said data storage device;</p>	<p>Trend Micro's software detects, using a process operating in kernel mode monitoring file system access, an attempt by the application to write data of a designated file type to said data storage device.</p> <p>As noted in the slides for limitation 1[pre], Trend Micro's software detects attempts by the applications to write data of a designated file type to said storage device.</p> <p>As shown below that detection can occur using a process operating in kernel mode monitoring files system access. For example, for behavior monitoring, Apex One and Office Scan use the Behavior Monitoring Core Driver which operates in kernel mode.</p> <div data-bbox="575 678 1709 1127" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Behavior Monitoring Components</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">COMPONENT</th><th>DESCRIPTION</th></tr> </thead> <tbody> <tr> <td>Behavior Monitoring Detection Pattern 32/64-bit</td><td>This pattern contains the rules for detecting suspicious threat behavior.</td></tr> <tr> <td>Behavior Monitoring Core Driver 32/64-bit</td><td>This <u>kernel mode</u> driver monitors system events and passes them to the Behavior Monitoring Core Service for policy enforcement.</td></tr> </tbody> </table> <p style="font-size: small; margin-top: 5px;">Trend Micro Apex One Administrator's Guide at 6-8</p> </div> <div data-bbox="621 1166 1709 1344" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr> <td style="width: 30%;">Behavior Monitoring Core Driver 32/64-bit</td><td>This <u>kernel mode</u> driver monitors system events and passes them to the Behavior Monitoring Core Service for policy enforcement.</td></tr> </tbody> </table> <p style="font-size: small; margin-top: 5px;">Office Scan, Service Pack 1, Administrator's Guide at 6-8</p> </div>	COMPONENT	DESCRIPTION	Behavior Monitoring Detection Pattern 32/64-bit	This pattern contains the rules for detecting suspicious threat behavior.	Behavior Monitoring Core Driver 32/64-bit	This <u>kernel mode</u> driver monitors system events and passes them to the Behavior Monitoring Core Service for policy enforcement.	Behavior Monitoring Core Driver 32/64-bit	This <u>kernel mode</u> driver monitors system events and passes them to the Behavior Monitoring Core Service for policy enforcement.
COMPONENT	DESCRIPTION								
Behavior Monitoring Detection Pattern 32/64-bit	This pattern contains the rules for detecting suspicious threat behavior.								
Behavior Monitoring Core Driver 32/64-bit	This <u>kernel mode</u> driver monitors system events and passes them to the Behavior Monitoring Core Service for policy enforcement.								
Behavior Monitoring Core Driver 32/64-bit	This <u>kernel mode</u> driver monitors system events and passes them to the Behavior Monitoring Core Service for policy enforcement.								



Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	TREND MICRO PRODUCTS						
16[a] detecting using a process operating in kernel mode monitoring file system access an attempt by the application to write data of a designated file type to said data storage device;	<p>As another example, Endpoint Application Control uses Kernel-Level Blocking process to monitor file system access and detect attempts by hostile applications to write data of designated file types to said storage device.</p> <div><p>Table 1. Blocking Methods</p><table><tr><th>Blocking Method</th><th>Action</th><th>Description</th></tr><tr><td><u>Kernel-level blocking</u> This method is sometimes also known as driver-level blocking.</td><td>Block applications before execution</td><td>Kernel-level blocking prevents applications from starting by blocking file access. This provides greater security, but may unexpectedly block or momentarily delay access to certain files needed by allowed applications. See About Kernel-Level Blocking.</td></tr></table><p>https://docs.trendmicro.com/en-us/enterprise/endpoint-application-control-20/rulesandpolicies/rulesandpoliciesabout/rulesblockmethods.aspx</p></div>	Blocking Method	Action	Description	<u>Kernel-level blocking</u> This method is sometimes also known as driver-level blocking.	Block applications before execution	Kernel-level blocking prevents applications from starting by blocking file access. This provides greater security, but may unexpectedly block or momentarily delay access to certain files needed by allowed applications. See About Kernel-Level Blocking .
Blocking Method	Action	Description					
<u>Kernel-level blocking</u> This method is sometimes also known as driver-level blocking.	Block applications before execution	Kernel-level blocking prevents applications from starting by blocking file access. This provides greater security, but may unexpectedly block or momentarily delay access to certain files needed by allowed applications. See About Kernel-Level Blocking .					

Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	TREND MICRO PRODUCTS																								
16[a] detecting using a process operating in kernel mode monitoring file system access an attempt by the application to write data of a designated file type to said data storage device;	<p>The excerpt below further shows the benefits of Endpoint Application Control’s Kernel-Level Blocking process, which shows monitoring attempts by designated file types to write data.</p> <div><p>Table 2. Blocking Method Benefits</p><table><tr><th>Benefit</th><th>Kernel-Level Blocking</th><th>User-Level Blocking</th></tr><tr><td>Prevents applications from starting before being evaluated</td><td>Yes</td><td></td></tr><tr><td>Blocks already-running applications</td><td></td><td>Yes</td></tr><tr><td><u>Compatible with all rule types</u></td><td>Yes</td><td>Yes</td></tr><tr><td><u>Blocks Windows Store applications</u></td><td>Yes</td><td>Yes</td></tr><tr><td><u>Blocks DLLs</u></td><td>Yes</td><td></td></tr><tr><td><u>Allows Trusted Sources</u></td><td>Yes</td><td></td></tr><tr><td>Preferred for timing-critical deployments, such as servers, trading systems, and manufacturing systems</td><td></td><td>Yes</td></tr></table><p>https://docs.trendmicro.com/en-us/enterprise/endpoint-application-control-20/rulesandpolicies/rulesandpoliciesabout/rulesblockmethods.aspx</p></div>	Benefit	Kernel-Level Blocking	User-Level Blocking	Prevents applications from starting before being evaluated	Yes		Blocks already-running applications		Yes	<u>Compatible with all rule types</u>	Yes	Yes	<u>Blocks Windows Store applications</u>	Yes	Yes	<u>Blocks DLLs</u>	Yes		<u>Allows Trusted Sources</u>	Yes		Preferred for timing-critical deployments, such as servers, trading systems, and manufacturing systems		Yes
Benefit	Kernel-Level Blocking	User-Level Blocking																							
Prevents applications from starting before being evaluated	Yes																								
Blocks already-running applications		Yes																							
<u>Compatible with all rule types</u>	Yes	Yes																							
<u>Blocks Windows Store applications</u>	Yes	Yes																							
<u>Blocks DLLs</u>	Yes																								
<u>Allows Trusted Sources</u>	Yes																								
Preferred for timing-critical deployments, such as servers, trading systems, and manufacturing systems		Yes																							

Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	TREND MICRO PRODUCTS
<p>16[b] in response to said attempt, retrieving a permission value from a database comprised of data elements encoding at least one permission value associated with the application; and</p>	<p>In response to the write attempts discussed for limitation 16[pre] and [a], Office Scan retrieves permission value from a database comprised of data elements encoding at least one permission value associated with the application. For example, the Behavior Monitoring functionality includes an exception list for approved programs and blocked programs. If a program is on the exception list as an approved program, Office Scan does not monitor that program. If a program is on the exception list as a blocked program, Office Scan blocks that program. Upon information and belief, the programs on the exception list are stored on a database that include data elements encoding permission values, e.g., approved or blocked, that are associated with the applications on the list.</p> <div data-bbox="764 636 1680 1349" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p style="text-align: center;"><u>Behavior Monitoring Exception List</u></p> <p>The Behavior Monitoring exception list contains programs that the OfficeScan agent does not monitor using Behavior Monitoring.</p> <ul style="list-style-type: none"> • <u>Approved Programs:</u> The OfficeScan agent allows all programs in the Approved Programs list to pass Behavior Monitoring scanning. <hr/> <div style="display: flex; align-items: flex-start;"> <div style="text-align: center; margin-right: 10px;">  <p>Note</p> </div> <p>Although Behavior Monitoring does not take action on programs added to the Approved Programs list, other scan features (such as file-based scanning) continue to scan the program before allowing the program to run.</p> </div> <hr/> <ul style="list-style-type: none"> • <u>Blocked Programs:</u> The OfficeScan agent blocks all programs in the Blocked Programs list. To configure the Blocked Programs list, enable Event Monitoring. <div style="text-align: right; margin-top: 20px;">  <p>9-9</p> </div> <p>Configure the exception list from the web console. You can also grant users the privilege to configure their own exception list from the OfficeScan agent console.</p> <p>For details, see Behavior Monitoring Privileges on page 9-19.</p> <p><small>Office Scan, Service Pack 1, Administrator's Guide at 9-9, 10.</small></p> </div>

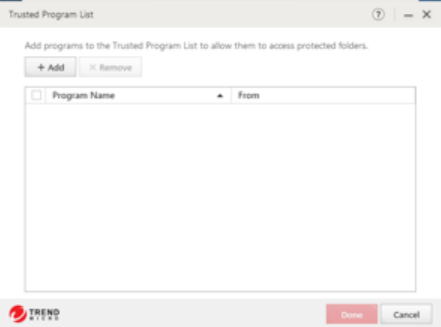
Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	TREND MICRO PRODUCTS
<p>16[b] in response to said attempt, retrieving a permission value from a database comprised of data elements encoding at least one permission value associated with the application; and</p>	<p>The Office Scan software also includes a Trusted Program list. Upon information and belief, the programs on that list are stored on a database that include data elements encoding permission values, e.g., trusted or not, that are associated with the applications on the list.</p> <div data-bbox="575 500 1593 823" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Trusted Program List</p> <p>You can configure OfficeScan agents to skip scanning of <u>trusted processes</u> during Real-time and Behavior Monitoring scans. After adding a program to the Trusted Programs List, the OfficeScan agent does not subject the program or any processes initiated by the program to Real-time Scan. Add trusted programs to the Trusted Program List to improve the performance of scanning on endpoints.</p> <p>Office Scan, Service Pack 1, Administrator's Guide at 9-2</p> </div>



Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	TREND MICRO PRODUCTS
<p>16[b] in response to said attempt, retrieving a permission value from a database comprised of data elements encoding at least one permission value associated with the application; and</p>	<p>Office Scan performs whitelist checking such as the exception list and trusted programs lists at each layer, i.e., at each the stages discussed on slide 3.</p> <div data-bbox="575 480 1728 1026" style="border: 1px solid black; padding: 10px;"> <ul style="list-style-type: none"> • Progressively filters out threats using the most efficient technique for maximum detection without false positives. • Blends signature-less techniques including high-fidelity machine learning, behavioral analysis, variant protection, census check, application control, exploit prevention, and good-file check with other techniques like file reputation, web reputation, and command and control (C&C) blocking. • Trend Micro is the first to infuse high-fidelity machine learning which uniquely analyzes files not only before execution but also during runtime for more accurate detection. • Noise cancellation techniques like census and <u>whitelist checking at each layer</u> reduce false positives. • Instantly shares information on suspicious network activity and files with other security layers to stop subsequent attacks. • Advanced ransomware protection monitors for suspicious file encryption activities at the endpoint, terminates malicious activities, and even recovers lost files if necessary. <p>Datasheet, Trend Micro Office Scan, at 2</p> </div>


Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	TREND MICRO PRODUCTS
<p>16[b] in response to said attempt, retrieving a permission value from a database comprised of data elements encoding at least one permission value associated with the application; and</p>	<p>Trend Micro's other software packages also include exception lists and trusted programs list. The following excerpt shows that Antivirus+ Security, Internet Security, and Maximum Security also include exception lists / trusted program lists.</p> <div data-bbox="573 485 1688 831" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p style="color: red; text-align: center;"><u>Exception Lists: Programs/Folders</u></p> <p style="text-align: center;">To add items to Exception Lists Programs/Folders:</p> <p>Trend Micro Security lets you add programs, folders, or websites to exception lists so that scans will ignore them. Adding programs or folders to exception lists can increase performance during scans, while adding frequently-accessed websites can prevent unwanted blockage. Users are advised to use exception lists wisely, as it may open computers up to more threats.</p> <p style="font-size: small;">Trend Micro Security 2020 for Windows Product Guide at 84.</p> </div> <div data-bbox="573 860 1463 1369" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>13. You can also click the link <u>Trusted Program List</u> to add a trusted program to a list of applications that can access protected folders. The Trusted Program List appears.</p>  <p style="text-align: center;">Figure 193. Trusted Program List</p> <p style="font-size: small;">Trend Micro Security 2020 for Windows Product Guide at 110-111.</p> </div>


Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	TREND MICRO PRODUCTS
<p>16[b] in response to said attempt, retrieving a permission value from a database comprised of data elements encoding at least one permission value associated with the application; and</p>	<p>The following excerpts also show that Apex One includes exception lists and trusted program lists.</p> <div data-bbox="558 415 1230 873" style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Behavior Monitoring <u>Exception List</u></p> <p>The Behavior Monitoring exception list contains programs that the Security Agent does not monitor using Behavior Monitoring.</p> <ul style="list-style-type: none"> • Approved Programs: The Security Agent allows all programs in the Approved Programs list to pass Behavior Monitoring scanning. <hr/> <p> Note</p> <p>Although Behavior Monitoring does not take action on programs added to the Approved Programs list, other scan features (such as file-based scanning) continue to scan the program before allowing the program to run.</p> <hr/> <ul style="list-style-type: none"> • Blocked Programs: The Security Agent blocks all programs in the Blocked Programs list. To configure the Blocked Programs list, enable Event Monitoring. <p>Configure the exception list from the web console. You can also grant users the privilege to configure their own exception list from the Security Agent console.</p> <p>For details, see Behavior Monitoring Privileges on page 9-18.</p> <p><small>Trend Micro Apex One Administrator's Guide at 9-9</small></p> </div> <div data-bbox="1251 415 1908 651" style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p><u>Trusted Program List</u></p> <p>You can configure Security Agents to skip scanning of trusted processes during Application Control, Behavior Monitoring, Data Loss Prevention, Device Control, Endpoint Sensor, and Real-time Scans. After adding a program to the Trusted Programs List, the Security Agent does not subject the program or any processes initiated by the program to Real-time Scan. Add trusted programs to the Trusted Program List to improve the performance of scanning on endpoints.</p> <p><small>Trend Micro Apex One Administrator's Guide at 7-51</small></p> </div> <div data-bbox="558 922 1268 1347" style="border: 1px solid black; padding: 5px;"> <p> Trend Micro Apex One™ Application Control™</p> <ul style="list-style-type: none"> • Prevents damage from unwanted/unknown applications (executables, DLLs, and other PE files). • Flexible, dynamic policies and <u>whitelisting/blacklisting</u> capabilities to reduce attack exposure. • Allows users to install applications based on reputation-based variables (prevalence, usage, and maturity). • Provides global and local real-time threat intelligence based on good file reputation data. • Categorizes applications and provides updates via our Trend Micro Certified Safe Software Service. • Coverage of pre-categorized applications that can be selected from our application catalog. • Visibility and policy management via Trend Micro Apex Central™. • Interconnects with additional layers of security to better correlate data and stop threats more often. <p><small>Trend Micro Apex One Administrator's Guide at 9-9</small></p> </div>

Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	TREND MICRO PRODUCTS
<p>16[b] in response to said attempt, retrieving a permission value from a database comprised of data elements encoding at least one permission value associated with the application; and</p>	<p>The following excerpts also show that, during for example real-time scans that run in response to a write attempt as discussed above, Office Scan and Apex One retrieve permission values from a database comprised of data elements encoding at least one permission value associated with the applications. Those permission values are stored on a database containing the Smart Scan Agent Pattern on the computer.</p> <div data-bbox="711 509 1717 1352" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p style="text-align: center;">Smart Scan Agent Pattern</p> <p>The Smart Scan Agent Pattern is updated daily and is <u>downloaded by the OfficeScan agents' update source</u> (the OfficeScan server or a custom update source). The update source then <u>deploys the pattern to smart scan agents</u>.</p> <hr/> <div style="display: flex; align-items: flex-start;">  <div> <p>Note</p> <p>Smart scan agents are OfficeScan agents that administrators have configured to use File Reputation Services. Agents that do not use File Reputation Services are called conventional scan agents.</p> </div> </div> <hr/> <p>Smart scan agents use the Smart Scan Agent Pattern when scanning for security risks. If the pattern cannot determine the risk of the file, another pattern, called Smart Scan Pattern, is leveraged.</p> <p style="text-align: center;">Smart Scan Pattern</p> <p>The Smart Scan Pattern is updated hourly and is downloaded by smart protection sources. Smart scan agents do not download the Smart Scan Pattern. Agents verify potential threats against the Smart Scan Pattern by sending scan queries to smart protection sources.</p> <p>Office Scan, Service Pack 1, Administrator's Guide at 4-8</p> </div>

Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	TREND MICRO PRODUCTS
<p>16[b] in response to said attempt, retrieving a permission value from a database comprised of data elements encoding at least one permission value associated with the application; and</p>	<p>The following excerpts shows the same Smart Scan Agent Pattern for the Apex One.</p> <div data-bbox="667 430 1703 1304" style="border: 1px solid black; padding: 10px;"> <p>Smart Scan Agent Pattern</p> <p>The Smart Scan Agent Pattern is updated daily and is <u>downloaded by the Apex One agents' update source</u> (the Apex One server or a custom update source). The update source then <u>deploys the pattern to smart scan agents</u>.</p> <hr/> <p> Note</p> <p>Smart scan agents are Security Agents that administrators have configured to use File Reputation Services. Agents that do not use File Reputation Services are called conventional scan agents.</p> <hr/> <p>Smart scan agents use the Smart Scan Agent Pattern when scanning for security risks. If the pattern cannot determine the risk of the file, another pattern, called Smart Scan Pattern, is leveraged.</p> <p>Smart Scan Pattern</p> <p>The Smart Scan Pattern is updated hourly and is downloaded by smart protection sources. Smart scan agents do not download the Smart Scan Pattern. Agents verify potential threats against the Smart Scan Pattern by sending scan queries to smart protection sources.</p> <p>Trend Micro Apex One Administrator's Guide at 4-8</p> </div>

Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	TREND MICRO PRODUCTS
<p>16[b] in response to said attempt, retrieving a permission value from a database comprised of data elements encoding at least one permission value associated with the application; and</p>	<p>Trend Micro’s Security software also uses a local database of permission values in combination with the online database of the Smart Protection Network. The signature database is maintained “mainly on Trend Micro Servers in the cloud,” which means that at least some of the database is stored locally.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 20px;"> <p>Unlike other local-protection-based products that require you to frequently update a large local signature database on your computer, Trend Micro Security <u>updates the signature database mainly on Trend Micro Servers in the cloud</u>, so all consumers of the Smart Protection Network are instantly protected whenever the online database is updated. Other cloud-based and local Trend Micro technologies correlate threat data of different kinds, since modern threats can simultaneously use multiple techniques to infect your computer.</p> <p>Smart Scan reduces network bandwidth usage (for updating/downloading signatures), while saving disk space and memory.</p> <p>Trend Micro Security 2020 for Windows Product Guide at 61.</p> </div>

Ex. E – Claim Chart
U.S. Patent No. 9,600,661

CLAIM 16	TREND MICRO PRODUCTS
<p>16[c] controlling write access to the data storage device by the application in dependence on said permission value.</p>	<p>As shown in the slides for limitation 16[c], Trend Micro's Software controls write access to the data storage device by the application in dependence on said permission value. For example, if the application is on the trusted programs list, approved programs list, or whitelist, then the application is allowed write access. If the application is on the blocked programs list or blacklist, then the application is denied write access.</p>